Protección de las empresas de atención sanitaria con Proofpoint

Protección de personas, procesos y datos de pacientes

Los ciberataques dirigidos contra el sector sanitario no han dejado de aumentar. Los datos extremadamente sensibles de los pacientes pueden tener un elevado valor económico, lo que convierte a estas empresas en un objetivo privilegiado para los ciberdelincuentes. La pandemia de COVID-19 ha convertido a este sector en todavía más vulnerable. El personal médico y no médico prestan ahora más servicios de atención al paciente de forma remota, lo que incrementa su exposición a las ciberamenazas. Proofpoint puede ayudarle. Nuestras soluciones de ciberseguridad y cumplimiento de normativas protegen su empresa, su plantilla y sus pacientes.

Las opciones de teleasistencia y teletrabajo son potentes herramientas que permiten al personal sanitario atender a los pacientes con total facilidad. Pero estas nuevas modalidades de trabajo abren la puerta a las ciberamenazas que podrían divulgar los datos médicos, perjudicar la asistencia a los pacientes o debilitar su seguridad.

Las instituciones sanitarias consideran ahora la ciberseguridad como un objetivo prioritario. Sin embargo, al igual que muchas empresas de otros sectores, han invertido en herramientas de seguridad tradicionales que protegen el perímetro de red. Estas herramientas no pueden ver (y mucho menos bloquear) las amenazas avanzadas que ponen en peligro los datos sanitarios.

Además, las amenazas evolucionan. A medida que el sector se desplaza fuera del perímetro de la red, también lo hacen los agresores. Pero las amenazas no solo se desplazan, también adoptan nuevas formas y objetivos. Cada persona de su organización de atención sanitaria representa un nivel diferente de seguridad o de riesgo de incumplimiento normativo. Este nivel se basa en los datos a los que tiene acceso cada una y en cómo utiliza la tecnología para hacer su trabajo.

El cuerpo de enfermería tiene mayor acceso a la información del paciente, lo que lo convierte en un objetivo prioritario. Los investigadores clínicos acceden a propiedad intelectual de gran valor, lo que aumenta considerablemente su nivel de vulnerabilidad. El personal hospitalario que trabaja en la cadena de suministro interacciona regularmente con varios sistemas externos, lo que aumentó considerablemente su nivel de vulnerabilidad. Las amenazas como el phishing de credenciales permiten a los ciberdelincuentes no solo hacerse con el control de una cuenta de correo electrónico, sino también acceder a gran cantidad de datos almacenados en la nube, fuera del alcance de las herramientas de seguridad tradicionales. A esta nueva variedad de ataques centrados en las personas están expuestos los trabajadores sanitarios, los pacientes y los médicos, entre otros.

Sin embargo, no debemos olvidar que las empresas de atención sanitaria siguen siendo un objetivo principal del ransomware y de otros ataques de malware. Estos ataques, sin bien no son muy numerosos, son ahora más dirigidos. Hoy más que nunca, las empresas deben continuar abordando este tipo de amenazas con una estrategia combinada de tecnología y formación.

Retos de ciberseguridad en el sector sanitario

Las organizaciones de atención sanitaria se enfrentan a nuevos retos en su búsqueda de estrategias innovadoras de prestación asistencial, sin poner en peligro su seguridad, la de sus médicos ni la de sus pacientes. En 2021 y en los próximos años, los problemas que afrontarán los responsables de TI y de seguridad tendrán mucha más complejidad, por lo que será aún más difícil para las instituciones sanitarias mantener un entorno seguro que posibilite la teleasistencia sanitaria.

Adopción de nuevos modelos asistenciales seguros

El uso de la asistencia móvil, la telemedicina y el Internet de las cosas ha aumentado la superficie de ataque. Los consumidores utilizan toda una variedad de aplicaciones de sanidad móvil, dispositivos médicos vestibles y tecnología médica domiciliaria. Los médicos llevan dispositivos personales al trabajo y dispositivos profesionales a casa. Además, las tecnologías emergentes y las fronteras difusas entre los parámetros clínicos y domésticos aumentan la complejidad. Todo ello ha contribuido a una transición hacia una infraestructura de TI descentralizada y sin perímetro mucho más difícil de proteger.

Almacenamiento y protección de datos

La protección de la relación médico-paciente es fundamental. Si los datos que se almacenan externamente no están seguros, o si se envían sin cifrar, la información de los pacientes puede quedar expuesta. Aunque todas las empresas sanitarias afirman recopilar, almacenar y compartir datos confidenciales, solo los cifra el 38 %[1].

Seguridad cloud

El sector sanitario es consciente de las numerosas ventajas que ofrece la nube: utilización de aplicaciones normalizadas, uso de modelos de pago por uso y reducción de gastos de capital. Habida cuenta de los riesgos derivados, el sector ha tardado en adoptar los servicios cloud, pero ahora está recuperando el tiempo perdido. Sin dejar de reconocer las ventajas evidentes de las soluciones cloud, los responsables de seguridad del sector de la atención sanitaria buscan propuestas capaces de garantizar el cumplimiento estricto de las normas, preservar la confidencialidad y la integridad de las transacciones, y que puedan adaptarse para proteger las aplicaciones cloud de sus socios comerciales y miembros de la cadena de suministro.

Paralelamente, muchas empresas de atención sanitaria siguen utilizando sistemas antiguos por la naturaleza propietaria de algunos de sus componentes, lo que les impide migrar a servicios cloud. Esta situación introduce otros riesgos, ya que los delincuentes aprovechan las nuevas vulnerabilidades para propagar malware (como ataques de ransomware) que puede dejar a las empresas fuera de línea.

Seguridad de la cadena de suministro

Los prestadores de asistencia sanitaria dependen de diversos proveedores externos, aliados y socios comerciales para garantizar sus actividades. Estas relaciones interdependientes forman un complejo ecosistema de terceros vulnerable al robo y a las ciberamenazas emergentes. Constituyen nuevos puntos de entrada que los ciberdelincuentes pueden aprovechar para comprometer la cadena de suministro de un hospital. Más que nunca, la seguridad en el sector sanitario se mide en el eslabón más débil de la cadena. Si se compromete un eslabón débil de la cadena de suministro de un hospital, puede utilizarse para extraer datos sensibles y las pérdidas pueden ser devastadoras.

Evolución del panorama de amenazas en el sector sanitario

El crecimiento del mercado de la información médica convierte a estas empresas en un atractivo blanco de ataque. Por lo tanto, deben adoptar un enfoque defensivo y asumir que el sector está bajo amenazas como el hacking y los ataques realizados por Estados. Los virus y el malware simples son cosa del pasado. Los ciberataques más devastadores están dirigidos a personas y son perpetrados por personas, que han localizado puntos de entrada a lo largo del tiempo, que, juntos, pueden provocar daños considerables. De hecho, según un informe, las empresas de atención sanitaria son las que más tardan en detectar una fuga de datos, con una media de 329 días[2].

1 2019 Thales Data Threat Report
(Informe de Thales sobre amenazas contra los datos, 2019)

2 Ponemon Institute, 2020 Cost of a Data Breach Report
(Informe sobre el coste de una fuga de datos, 2020), publicado por IBM Security

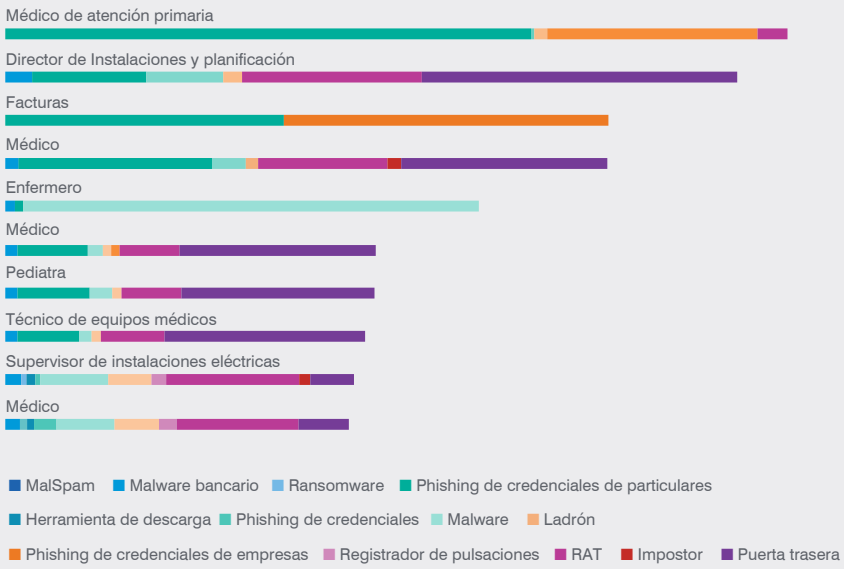

Figura 1: Distribución de VAP en un prestigioso hospital infantil.

Adopción de una estrategia centrada en las personas

Los ciberataques actuales tienen como objetivo a las personas, no a la tecnología. Por eso, las empresas de atención sanitaria deben adoptar una estrategia centrada en las personas que proteja a sus trabajadores médicos, sus empleados no médicos y los datos sensibles que estos utilizan y comparten. La naturaleza del trabajo médico exige centrarse en prestar, normalmente con rapidez, una atención óptima al paciente, y no en considerar la legitimidad de un mensaje de correo electrónico. Esta es una de las razones por las que el sector sigue siendo un objetivo fácil para los ciberdelincuentes. Además, las ganancias potenciales en caso de éxito del ataque son elevadas.

Al mismo tiempo, las organizaciones de atención sanitaria deben satisfacer los estrictos requisitos del Reglamento general de protección de datos (RGPD) de la UE, especialmente porque tratan y almacenan datos genéticos, biométricos y médicos (categorías todas ellas incluidas en la lista de datos considerados como sensibles), con los que es preciso implementar un mayor nivel de control. Las empresas deben aplicar controles de seguridad adecuados para proteger sus datos, no solo para evitar posibles sanciones, sino también para salvaguardar la privacidad de los pacientes.

Nuestro informe de 2020, "El panorama de las amenazas en el sector sanitario", analiza lo que denominamos VAP (Very Attacked People™, o personas muy atacadas) en el sector. Utilizamos este término para describir a los usuarios de una organización que son los objetivos más prioritarios de las ciberamenazas. La figura 1 muestra un ejemplo ocurrido en la realidad.

Hospital infantil

En este ejemplo, el cargo más atacado fue el de "médico". Las preocupaciones por la privacidad son incluso mayores en el caso de los menores, ya que son un objetivo muy atractivo para los robos de identidad. La historia clínica de un paciente menor de edad es extremadamente valiosa en la web oscura o el mercado clandestino. La mayoría de los niños no cuentan con un historial crediticio y no van a solicitar préstamos ni tarjetas de crédito. Los ciberdelincuentes saben que, en el momento del ataque, la mayoría de nosotros no estamos supervisando si sus datos se utilizan para cometer fraudes. En concreto, el volumen de actividad de puertas traseras fue superior en el departamento de gestión de instalaciones, que suele tener controles de seguridad más relajados.

Normalmente, estos entornos emplean recursos permisivos, como dispositivos del Internet de las cosas (IoT) y sistemas de filtración de aire, que a menudo se utilizan como puntos de acceso a la red para atacar la infraestructura de TI de la empresa.

Casos de uso del sector sanitario

Seguridad distribuida

La atención sanitaria abarca una amplia gama de organizaciones y entornos de TI que comparten información entre pacientes y médicos para migrar hacia un modelo de asistencia conectada o centrada en el paciente. El correo electrónico es un método frecuente de divulgar información confidencial, por lo que una gran mayoría de las fugas destacadas de datos sanitarios comienzan por ataques dirigidos de phishing.

Proofpoint posee las soluciones adecuadas para que el sector sanitario proteja a los usuarios del modo en el que trabajan en la actualidad:

- **Proofpoint Email Protection** es una potente solución de seguridad del correo electrónico que permite bloquear el malware y otras amenazas.
- **Proofpoint Data Loss Prevention (DLP)** limita el riesgo de pérdida de datos y protege frente a las estafas por correo electrónico.
- **Proofpoint Targeted Attack Protection (TAP)** integra funciones de entorno aislado (sandbox) que permiten detectar y bloquear las amenazas avanzadas.
- **Proofpoint Threat Response** permite a las empresas reaccionar con rapidez para neutralizar las amenazas y eliminar los mensajes de correo electrónico maliciosos.
- **Proofpoint Security Awareness Training** proporciona formación que permite a los empleados aprender a identificar los ataques de ingeniería contra el sector sanitario, como las técnicas sofisticadas de phishing.

Protección contra ataques de impostores

Los mensajes de correo electrónico fraudulentos son mensajes diseñados para hacerse pasar por una persona que el destinatario conoce o en quien puede confiar. Estos ataques pueden ser difíciles de detectar porque no se aprovechan de vulnerabilidades técnicas. Están dirigidos a cargos específicos que tienen acceso a actividad monetizable, como farmacéuticos, investigadores clínicos, trabajadores de la cadena de suministro o personal de base del hospital.

Proofpoint ofrece una solución global, integral y centrada en las personas que bloquea todas las formas de fraude por correo electrónico, sea cual sea la táctica utilizada o la persona atacada:

- La solución de **seguridad avanzada del correo electrónico** de Proofpoint bloquea los mensajes de correo electrónico de phishing y de impostores que suplantan nombres de dominio o utilizan nombres parecidos. Emplea técnicas avanzadas de aprendizaje automático y múltiples motores de detección para localizar estos ataques dirigidos y los detiene antes de que lleguen a la bandeja de entrada de los usuarios.
- El protocolo **DMARC (Domain-based Message Authentication Reporting and Conformance)** se despliega para facilitar la autenticación de los mensajes de correo electrónico. Bloquea los mensajes falsificados antes de que los empleados, el personal clínico y los socios comerciales sean víctimas de un fraude.

Protección de Microsoft 365 y de otros entornos cloud

Una solución CASB (Cloud Access Security Broker) constituye un elemento esencial de toda arquitectura de seguridad cloud. Cada vez más las empresas de atención sanitaria migran datos y aplicaciones a la nube y acceden a los datos más sensibles a través de conexiones a Internet. Necesitan una visibilidad de las actividades cloud en todo el ecosistema sanitario y la cadena de suministro.

Proofpoint CASB ayuda a las organizaciones a realizar análisis y a neutralizar con rapidez las violaciones de reglas de mensajería cloud para garantizar la continuidad de la asistencia médica. Reduce el riesgo de ciberataques o fugas de datos y utiliza el flujo de correo electrónico corporativo para identificar datos confidenciales en los servicios de alojamiento de archivos en la nube, como Microsoft 365, Dropbox, Box y Salesforce.

Colaboración asistencial segura

El personal sanitario necesita colaborar y comunicarse con eficacia en el centro de atención. Para ello, dispone de soluciones móviles que conectan a los médicos y a los pacientes, pero que están diseñadas pensando en la funcionalidad y la comodidad, no en la seguridad. Además, a menudo se utilizan fuera de los límites de la red empresarial protegida.

Los médicos pueden acceder a aplicaciones clínicas desde sus dispositivos personales y también utilizar cuentas de correo electrónico personales en el hardware de la empresa. **Proofpoint Browser Isolation** mantiene las actividades personales y el contenido peligroso fuera de su entorno.

Funciona aislando en un contenedor protegido el correo web y todas las URL que incluyan. Los usuarios pueden acceder a sus cuentas personales con libertad y privacidad a través de su navegador web habitual. Sin embargo, las acciones y el contenido potencialmente peligrosos se desactivan, para preservar así la seguridad de su entorno.

Protección frente a amenazas internas

Un empleado interno que filtre información sobre pacientes de la consulta de un médico o de un hospital es una escena digna de una serie de televisión. Pero las amenazas internas son bien reales. De hecho, casi en la mitad de las fugas que se producen en el sector sanitario está implicado un usuario interno[3].

Estas son las tres amenazas internas más habituales en las empresas de atención sanitaria:

1. Robo o uso indebido de la información sanitaria
2. Robo o uso indebido de historiales médicos electrónicos
3. Fraudes de seguros y otros fraudes financieros

Insider Threat Management (ITM) de Proofpoint protege contra las fugas de datos, los actos maliciosos y los daños a la marca debidas a la mala intención, a la negligencia o al desconocimiento de los usuarios internos. Nuestra solución ITM correlaciona las actividades y los movimientos de datos, lo que permite a los equipos de seguridad identificar los riesgos asociados a los usuarios, detectar y responder a las fugas de datos provocadas por usuarios internos, y acelerar la respuesta a incidentes de seguridad.

3 Verizon, 2020 Data Breach Investigations Report Informe de Verizon sobre las investigaciones de fugas de datos, 2020)

Protección de la información sanitaria: cómo garantizar la seguridad de los datos de los pacientes

En el sector de la salud, el correo electrónico constituye el principal vector de amenazas. Contar con la solución más adecuada de prevención de pérdida de datos (DLP) del correo electrónico es la garantía de que solo las personas apropiadas clasifiquen y accedan a la información sensible y estratégica.

Gracias a **la solución DLP centrada en las personas de Proofpoint**, las empresas de atención sanitaria pueden identificar y neutralizar con rapidez los riesgos asociados a usuarios negligentes, maliciosos o cuyas cuentas están comprometidas. La plataforma unificada de Proofpoint permite a los clientes definir los datos de interés, aplicar estas definiciones en toda la plataforma de Proofpoint y proteger la confidencialidad de los mensajes de correo electrónico a través de **Email Encryption**. Los usuarios pueden activar automáticamente el cifrado de mensajes añadiendo al asunto una clave de su elección o bien activar el cifrado basándose en reglas DLP.

El gestor de incidentes unificado de Proofpoint no solo representa un punto único para ver las infracciones de reglas DLP en todo el correo electrónico, el entorno cloud y los endpoints, sino que, al combinar estos datos, también proporciona amplia información sobre las amenazas y el contexto.

Administración del cumplimiento de normativas y reducción de la complejidad

Numerosas empresas reguladas tienen problemas para:

- Identificar los canales de comunicación utilizados
- Asegurar que el contenido de esas comunicaciones se captura y archiva con total seguridad
- Buscar y recuperar contenido para auditorías de manera rápida y rentable
- Supervisar y controlar a los trabajadores que utilizan estos canales

La solución de **archivado y cumplimiento de normativas de Proofpoint** ofrece cumplimiento todo en uno centrado en las personas.

Disfrutará de las siguientes ventajas:

- Estará protegido desde el momento en que el contenido se difunde hasta el momento en que se indexa, archiva y recupera.
- Sus políticas reguladoras se aplicarán automáticamente, concretamente las normativas locales en materia de sanidad y las relativas al RGPD.
- Tendrá la seguridad de que su actividad de interacción digital cumple todas las normas de comunicación y retención.
- Podrá supervisar, corregir (revisar o eliminar) y archivar contenido fácil, rápida y económicamente.

Conclusión

Proofpoint proporciona a las instituciones de atención sanitaria protección y visibilidad ante el mayor riesgo para su ciberseguridad: las personas. Proporcionamos la ciberseguridad más eficaz para proteger a los profesionales de la sanidad frente a ataques de toda procedencia, ya sean a través del correo electrónico, la web, las redes sociales o las aplicaciones cloud. Ayudamos al sector sanitario a bloquear las amenazas antes de que lleguen al personal clínico y auxiliar, a salvaguardar los datos y, en última instancia, a proteger a los pacientes frente a los ciberataques. Importantes organizaciones sanitarias de todos los tamaños confían en Proofpoint para prevenir, detectar y neutralizar las amenazas más críticas antes de que causen daños duraderos.

MÁS INFORMACIÓN

Para obtener más información sobre cómo podemos ayudarle a adoptar una estrategia centrada en las personas para proteger sus datos, operaciones y atención sanitaria, visite **proofpoint.com/us/solutions/healthcare-information-security.**